

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method for authenticating a ~~computer~~ computing device, the method comprising the following steps:

issuing a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from a first ~~computer~~ computing device to a second ~~computer~~ computing device;

transmitting said credential and a computer challenge from the second ~~computer~~ computing device to the first ~~computer~~ computing device when the second ~~computer~~ computing device is to be authenticated;

transmitting a response to said computer challenge from said first ~~computer~~ computing device to said second ~~computer~~ computing device; and

verifying said response with said second ~~computer~~ computing device in order to authenticate and verify said ~~computers~~ computing devices.

2. (Currently Amended) The method of claim 1 wherein the challenge is a random number generated by the second ~~computer~~ computing device and the first ~~computer~~ computing device computes the response to the challenge by performing a predetermined function on the random number.

3. (Currently Amended) The method of claim 2 wherein the second ~~computer~~ computing device determines whether the first ~~computer~~ computing device response is valid by performing the predetermined function on the random number and comparing the result to the response.

4. (Original) The method of claim 3 wherein the predetermined function is a hash function.

5. (Currently Amended) The method of claim 1 wherein the second ~~computer~~ computing device establishes a connection with the first ~~computer~~ computing device when the response is valid.

6. (Currently Amended) The method of claim 1 wherein the first ~~computer~~ computing device determines whether the credential transmitted from the second ~~computer~~ computing device is valid by determining whether the expiration time of the credential has been exceeded.

7. (Currently Amended) A system for authenticating a computer, the system comprising:

a first computer; and

a second computer in communication with the first computer;

wherein the first computer and the second computer are configured to execute the following instructions:

issue a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from the first computer to the second computer;

transmit the credential and a challenge from the second computer to the first computer when the second computer is to be authenticated;

transmit a response to the challenge from the first computer to the second computer; and

verify the response with the second computer in order to authenticate and verify the computers.

8. (Original) The system of claim 7 wherein the second computer is configured to generate a challenge that is a random number and the first computer is configured to generate a response to the challenge by performing a predetermined function on the random number.

9. (Original) The system of claim 8 wherein the second computer is configured to determine whether the response is valid by performing the predetermined function on the random number and comparing the result to the response.

10. (Original) The system of claim 9 wherein the predetermined function is a hash function.

11. (Original) The system of claim 7 wherein the second computer establishes a connection with the first computer when the response is valid.

12. (Previously Presented) The system of claim 7 wherein the first computer determines whether the credential transmitted from the second computer is valid by determining whether the expiration time of the credential has been exceeded.

13. (Currently Amended) A method for authenticating a computer, the method comprising the steps:

issuing a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from a first computer to a second computer;

generating with the second computer a first challenge;

transmitting the credential and the first challenge from the second computer to the first computer;

determining with the first computer whether the credential is valid;

computing a first response to the first challenge and generating a second challenge with the first computer;

transmitting the first response and the second challenge from the first computer to the second computer;

determining with the second computer whether the first response is valid;

computing a second response to the second challenge with the second computer;

transmitting the second response from the second computer to the first computer; and

determining with the first computer whether the second response is valid to verify and authenticate the computers.

14. (Original) The method of claim 13 wherein the second computer encrypts the credential before transmitting the credential to the first computer.

15. (Original) The method of claim 13 wherein the first computer challenge is a random number generated by the second computer and the first computer computes a first response to the first challenge by performing a predetermined function on the random number.

16. (Original) The method of claim 15 wherein the second computer determines whether the first response is valid by performing the predetermined function on the random number and comparing the result to the first response.

17. (Original) The method of claim 15 wherein the predetermined function is a hash function.

18. (Original) The method of claim 13 wherein the second challenge is a random number generated by the first computer and the second computer computes a second response to the second challenge by performing a predetermined function on the random number.

19. (Original) The method of claim 18 wherein the first computer determines whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

20. (Original) The method of claim 19 wherein the predetermined function is a hash function.

21. (Previously Presented) The method of claim 13 wherein the first computer determines whether the credential transmitted from the second computer is valid by determining whether the expiration time of the credential has been exceeded.

22. (Original) The method of claim 13 further comprising the steps of:
encrypting the first challenge with the second computer before transmitting to the first computer;

decrypting the first challenge with the first computer before determining whether the first response is computed;

encrypting the first response and the second challenge with the first computer before transmitting;

decrypting the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypting the second response with the second computer before transmitting; and

decrypting the second response with the first computer before determining whether the second response is valid.

23. (Original) The method of claim 22 wherein the credential is encrypted before issuing the credential to the second computer and the credential is decrypted by the first computer when returned by the second computer.

24. (Currently Amended) A computer-readable medium containing a program with instructions that execute the following procedure:

issue a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from a first computer to a second computer;

generate a first challenge with the second computer;

transmit the credential and the first challenge from the second computer to the first computer;

determine with the first computer whether the credential is valid;

compute a first response to the first challenge and generate a second challenge with the first computer;

transmit the first response and the second challenge from the first computer to the second computer;

determine with the second computer whether the first response is valid to verify the first computer;

compute a second response to the second challenge with the second computer;
transmit the second response from the second computer to the first computer;
and
determine with the first computer whether the second response is valid to verify and authenticate the computers.

25. (Original) The computer-readable medium of claim 24 having instructions for the second computer to encrypt the credential before transmitting the credential to the first computer.

26. (Original) The computer-readable medium of claim 24 having instructions for the second computer to generate the first challenge that is a random number and the first computer computes a first response to the first challenge by performing a predetermined function on the random number.

27. (Original) The computer-readable medium of claim 26 wherein the second computer determines whether the first response is valid by performing the predetermined function on the random number and comparing the result to the first response.

28. (Original) The computer-readable medium of claim 27 wherein the predetermined function is a hash function.

29. (Original) The computer-readable medium of claim 24 having instructions for the first computer to generate a second challenge that is a random number and the second computer computes a second response to the second challenge by performing a predetermined function on the random number.

30. (Original) The computer-readable medium of claim 29 wherein the first computer determines whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

31. (Original) The computer-readable medium of claim 30 wherein the predetermined function is a hash function.

32. (Previously Presented) The computer-readable medium of claim 24, wherein the first computer determines whether the credential transmitted from the second computer is valid by determining whether the expiration time of the credential has been exceeded.

33. (Original) The computer-readable medium of claim 24 further comprising instructions for:

encrypting the first challenge with the second computer before transmitting to the first computer;

decrypting the first challenge with the first computer before the first response is computed;

encrypting the first response and the second challenge with the first computer before transmitting;

decrypting the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypting the second response with the second computer before transmitting; and

decrypting the second response with the first computer before determining whether the second response is valid.

34. (Original) The computer-readable medium of claim 33 wherein the instructions further comprise encrypting the credential before issuing the credential to the second computer and decrypting the credential with the first computer when returned from the second computer.

35. (Currently Amended) A system for authenticating a computer, the system comprising:

a first computer; and

a second computer in communication with the first computer;

wherein the first computer and the second computer are configured to execute the following instructions:

issue a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from the first computer to the second computer;

generate a first challenge with the second computer;
transmit the credential and the first challenge from the second
computer to the first computer;
determine with the first computer whether the credential is valid;
compute a first response to the first challenge and generate a second
challenge with the first computer;
transmit the first response and the second challenge from the first
computer to the second computer;
determine with the second computer whether the first response is valid;
compute a second response to the first challenge with the second computer;
transmit the second response from the second computer to the first
computer; and
determine with the first computer whether the second response is valid
to authenticate and verify the computers.

36. (Original) The system of claim 35 wherein the second computer is configured to encrypt the credential before transmitting the credential to the first computer.

37. (Original) The system of claim 35 wherein the second computer is configured to generate a first challenge that is a random number and the first computer is configured to compute a first response to the first challenge by performing a predetermined function on the random number.

38. (Original) The system of claim 37 wherein the second computer is configured to determine whether the first response is valid by performing the predetermined function on the random number and compare the result to the first response.

39. (Original) The system of claim 38 wherein the predetermined function is a hash function.

40. (Original) The system of claim 35 wherein the first computer is configured to generate a second challenge that is a random number and the second computer is configured to compute a second response to the second challenge by performing a predetermined function on the random number.

41. (Original) The system of claim 40 wherein the first computer is configured to determine whether the second response is valid by performing the predetermined function on the random number and comparing the result to the second response.

42. (Original) The system of claim 41 wherein the predetermined function is a hash function.

43. (Previously Presented) The system of claim 35 wherein the first computer is configured to determine whether the credential transmitted from the

second computer is valid by determining whether the expiration time of the credential has been exceeded.

44. (Original) The system of claim 35 wherein the first computer and the second computer are configured to:

encrypt the first challenge with the second computer before transmitting to the first computer;

decrypt the first challenge with the first computer before the first response is computed;

encrypt the first response and the second challenge with the first computer before transmitting;

decrypt the first response and the second challenge with the second computer before determining whether the first response is valid and the second response is computed;

encrypt the second response with the second computer before transmitting;
and

decrypt the second response with the first computer before determining whether the second response is valid.

45-47. (Canceled)

48. (Currently Amended) A method of authentication performed between a first user and a second user with a computer, the method comprising the steps of:

issuing a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from the first user to the second user;

generating a first challenge with the second user;

transmitting the credential and the first challenge to the first user;

determining with the first user whether the credential is valid;

generating with the first user a first response to the first challenge and a second challenge;

transmitting the first response and the second challenge to the second user;

determining with the second user whether the first response is valid;

generating with the second user a second response to the second challenge;

transmitting the second response to the first user; and

determining with the first user whether the second response is valid in order to authenticate and verify the first and second users.

49. (Currently Amended) A method for authenticating a computer, the method comprising the following steps:

issuing a credential based on session information, a hash seed, a maximum iterative value ~~security parameters~~, credential information and an expiration time from a first computer to a second computer;

in response to a connection between the first computer and the second computer being terminated, transmitting said credential and a computer challenge from the second computer to the first computer when the second computer is to be authenticated;

transmitting a response to said computer challenge from said first computer to said second computer; and

verifying at said second computer whether said response is valid, wherein said second computer re-establishes a connection with the first computer when the response is valid.

50. (Previously Presented) The method of claim 49, wherein the challenge comprises a random number generated by the second computer, wherein the first computer generates the response to the challenge by calculating a predetermined function of the random number, and wherein the second computer verifies whether the response is valid by calculating the predetermined function of the random number and comparing the result of the calculation to the response.

51. (Previously Presented) The method of claim 49, the method further comprising:

checking at the first computer whether the credential transmitted from the second computer is valid by determining whether the expiration time of the credential has been exceeded.